



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/838,759	04/19/2001	Lance W. Russell	10003536-1	1330
7590	05/05/2006		EXAMINER	
HEWLETT-PACKARD COMPANY Intellectual Property Administration P.O. Box 272400 Fort Collins, CO 80527-2400			KLIMACH, PAULA W	
			ART UNIT	PAPER NUMBER
			2135	

DATE MAILED: 05/05/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)
	09/838,759	RUSSELL ET AL.
	Examiner	Art Unit
	Paula W. Klimach	2135

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --
Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).

Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1) Responsive to communication(s) filed on 02 February 2006.

2a) This action is FINAL. 2b) This action is non-final.

3) Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4) Claim(s) 1,2,8 and 13 is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5) Claim(s) _____ is/are allowed.

6) Claim(s) 1,2,8 and 13 is/are rejected.

7) Claim(s) _____ is/are objected to.

8) Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9) The specification is objected to by the Examiner.

10) The drawing(s) filed on _____ is/are: a) accepted or b) objected to by the Examiner.
 Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
 Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11) The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12) Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
 a) All b) Some * c) None of:
 1. Certified copies of the priority documents have been received.
 2. Certified copies of the priority documents have been received in Application No. _____.
 3. Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) Notice of References Cited (PTO-892)
 2) Notice of Draftsperson's Patent Drawing Review (PTO-948)
 3) Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
 Paper No(s)/Mail Date 08/09; 01/05.

4) Interview Summary (PTO-413)
 Paper No(s)/Mail Date. _____.
 5) Notice of Informal Patent Application (PTO-152)
 6) Other: _____.

DETAILED ACTION

Response to Amendment

This office action is in response to amendment filed on 02/02/06. The amendment filed on 02/02/06 have been entered and made of record. Therefore, presently pending claims are 1, 2, 8, and 13.

Response to Arguments

Applicant's arguments filed 02/02/06 have been fully considered but they are not persuasive because of following reasons.

As discussed during the telephonic interview the use of partial keys in a distributed system does not create a distinction over the prior art. However the use of the distributed file interface in the encryption/decryption process as recited in claim 3 combined with the claim language as disclosed in currently amended claims 1 and 13 would distinguish the application over the prior art.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

Claims 1 and 13 are rejected under 35 U.S.C. 103(a) as being unpatentable over Moore (6,678,700) in view of Moskowitz (20020071556 A1), Kaplan (IBM Cryptolopes,

SuperDistribution and Digital Rights Management) and further in view of the article by Bellare et al.

In reference to claims 1 and 13, Moore et al (6,678,700) discloses a method of receiving at the meta-data server an open-file request that is created by the application (distributed file interface coupled to the client; column 6 lines 36-45), the open-file request specifying a name of a first file, wherein the first file includes a first set of blocks (column 6 lines 13-45 in combination with column 18 lines 23-28). The request for the resource would include the name of the file (Fig. 7 part 40). During the creation of the Meta data creation of normal objects is used to put data objects into a container at the SRB server (meta data server) (column 18 lines 37-46), thus creating an object in response to the open-file request. Moore discloses writing the data to the copy then updating the container. This is the function of transmitting the object to the file interface because the client and the server have the same copy of the information on the file interface.

However Moore does not disclose generating an encryption key at the meta-data server and the storage server.

Moskowitz et al teaches the generation of partial keys at different entities (page 3 paragraph 0023). The first key creator creates the first part of the key and corresponds to the meta-data server and the second key creator creates the second part of the key and corresponds to the storage server (page 2 paragraph 0015).

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to use partial keys created at different servers as in the system of Moskowitz and

adding the keys to the data portion of the object in the system of Moore, thus creating a security object. One of ordinary skill in the art would have been motivated to do this because sharing the secret between more devices increases the amount of security since both values are required for decrypting the message.

Moore and Moskowitz do not disclose adding the generated keys and the block list to the security object.

The system of the Kaplan discloses a system for digital rights management that comprises a distributed file system (Fig on page 6). The system adds the block list, which corresponds to the lists of parts, to the security object (Bill of Materials page 5 paragraph 3). The security object is transmitted to a distributed file interface (paragraph 3 page 6).

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to store the key of Moskowitz and the list in the security object, Cryptolope, of Kaplan within the network of Moore. One of ordinary skill in the art would have been motivated to do this because it would protect content and track its usage, and to fairly and efficiently distribute royalties and licensing fees (SuperDistribution of Cryptolopes to the rescue... page 1).

The list of Kaplan is not encrypted, however at the time the invention was made, it would have been obvious to a person of ordinary skill in the art to encrypt the list of parts for the cryptolope. One of ordinary skill in the art would have been motivated to do this because it adds more security to the authentication of the information for a cryptolope, since only the person with the key would be able to encrypt the system so that authentic key users can decrypt the list and therefore authenticate the contents; and further the cryptolope is encrypted therefore it is just one more level of encryption.

The system discussed by Kaplan performs the transmission of the security object form server to server, furthermore the system of Moore discloses the Meta-data server that contains the data files. Moskowitz discloses systems that create the key that is used for encryption.

The article of Bellare discloses a system that utilizes and generates partial keys that are sent to the systems involved in the encryption process (pages 78-88).

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to utilize the partial keys of Bellare in the system of Moore. One of ordinary skill in the art would have been motivated to do this because the would ensure the agreement of all parties in the encryption and decryption process.

Claims 2 and 8 are rejected under 35 U.S.C. 103(a) as being unpatentable over Moore, Moskowitz, and Kaplan as applied to claim 1 above, and further in view of Brundrett et al. (6,249,866).

In reference to claim 2, Moore discloses transmitting a file access request and security object from the distributed file system interface to the storage server in response to a file access request from a client application (column 6 lines 36-48), the file access request including an operation code and a reference to selected data of a file (column 19 lines 33-39);

Moore and Moskowitz do not disclose decrypting the block list at the storage server in response to the file access request; providing access to the selected data in accordance with the operation code upon successful decryption of the block list.

Brundrett discloses decrypting the text for the NTFS in response from a request from an application and thereby providing access to the selected data upon successful decryption (column 17 lines 6-34).

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to decrypt the file as in Brundrett in the system of Moore. One of ordinary skill in the art would have been motivated to do this because decryption makes the encrypted data available to the user.

In reference to claims 3, 8, Brundrett further discloses encrypting file data at the distributed file interface for file write operations using the encryption key in the security object; and decrypting file data at the distributed file interface for file read operations using the encryption key in the security object (Fig. 17 and Fig. 20).

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to encrypt the file as in Brundrett and adding the encrypted information to the data portion of the object in the system of Moore. One of ordinary skill in the art would have been motivated to do this because encryption secures the information.

Allowable Subject Matter

Claims 3-7, and 9-12 are objected to as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims.

Claims 14-16 are allowed.

Art Unit: 2135

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Paula W. Klimach whose telephone number is (571) 272-3854. The examiner can normally be reached on Mon to Thr 9:30 a.m to 5:30 p.m.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached on (571) 272-3859. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

PWK

Monday, May 01, 2006

H.T. Song
HOSUK SONG
PRIMARY EXAMINER